

SK/MTK/AFM  
F.#2016R02228

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

----- X

UNITED STATES OF AMERICA

- against -

No. 18-CR-633 (S-1) (EK)

ALEKSANDR ZHUKOV,  
also known as “Alexander  
Zhukov” and “ibetters,”

Defendant.

----- X

THE GOVERNMENT’S SUPPLEMENTAL MOTIONS IN LIMINE

SETH D. DUCHARME  
ACTING UNITED STATES ATTORNEY  
Eastern District of New York  
271 Cadman Plaza East  
Brooklyn, New York 11201

Saritha Komatireddy  
J. Artie McConnell  
Alexander F. Mindlin  
Assistant U.S. Attorneys  
(Of Counsel)

TABLE OF CONTENTS

PRELIMINARY STATEMENT .....	1
BACKGROUND .....	2
ARGUMENT .....	5
I. The Court Should Admit Evidence of the Defendant's Other Acts Pursuant to Federal Rule of Evidence 404(b) .....	5
II. The Court Should Admit the LinkedIn Profiles of Certain of the Defendant's Uncharged Co-Conspirators .....	8
III. The Court Should Order the Defense to Provide a More Complete Expert Disclosure .....	133
IV. The Court Should Permit the Government to Cross-Examine the Defense Expert On His Prior Conviction .....	155
CONCLUSION .....	200

TABLE OF AUTHORITIESCASES

<u>Huddleston v. United States</u> , 485 U.S. 681 (1988).....	13
<u>In re Terrorist Bombings of U.S. Embassies in East Africa</u> , 552 F.3d 93 (2d Cir. 2008).....	17
<u>United States v. Alvarado</u> , 882 F.2d 645 (2d Cir. 1989).....	8
<u>United States v. Aminy</u> , 15 F.3d 258 (2d Cir. 1994).....	13
<u>United States v. Amodeo</u> , 44 F.3d 141 (2d Cir. 1995).....	5
<u>United States v. Beech-Nut Nutrition Corp.</u> , 871 F.2d 1181 (2d Cir. 1989).....	18
<u>United States v. Black</u> , No. 13-CR-316 (DLI), 2014 WL 5783067 (E.D.N.Y. Nov. 5, 2014)	7
<u>United States v. Blake</u> , 195 F. Supp. 3d 605 (S.D.N.Y. 2016) .....	8
<u>United States v. Carboni</u> , 204 F.3d 39 (2d Cir. 2000).....	13
<u>United States v. Davidson</u> , 308 F. Supp. 2d 461 (S.D.N.Y. 2004).....	7
<u>United States v. Dupree</u> , 706 F.3d 131, 136 (2d Cir. 2013).....	11, 13
<u>United States v. Fawwaz</u> , 691 F. App'x 676 (2d Cir. June 2, 2017).....	8
<u>United States v. Fawwaz</u> , No. 15 CR 1731, 2017 WL 2399329 (2d Cir. June 2, 2017).....	18
<u>United States v. Germosen</u> , 139 F.3d 120 (2d Cir. 1998) .....	13
<u>United States v. Gigante</u> , 166 F.3d 75 (2d Cir.1999) .....	17
<u>United States v. Glover</u> , 101 F.3d 1183 (7th Cir. 1996).....	9
<u>United States v. Gonzalez</u> , 399 F. App'x 641 (2d Cir. 2016).....	8
<u>United States v. Gupta</u> , 747 F.3d 111 (2d Cir. 2014).....	8, 9
<u>United States v. Harper</u> , No. 05-CR-6068, 2009 WL 140125 (W.D.N.Y. Jan. 20, 2009) .....	8
<u>United States v. Hill</u> , 658 F. App'x 600 (2d Cir. 2016) .....	7
<u>United States v. Jackson</u> , 180 F.3d 55 (2d Cir. 1999) .....	10
<u>United States v. Johnson</u> , 507 F.3d 793 (2d Cir. 2007).....	7, 8, 9

<u>United States v. Lange</u> , 834 F.3d 58 (2d Cir. 2016).....	8
<u>United States v. Mahaffy</u> , No. 05-CR-613 (S-3) (ILG), 2007 WL 1094153 (E.D.N.Y. Apr. 10, 2007) .....	11
<u>United States v. Marin</u> , 669 F.2d 73 (2d Cir. 1982).....	7, 10
<u>United States v. Mitchell</u> , 502 F.3d 931 (9th Cir. 2007) .....	7
<u>United States v. Pitre</u> , 960 F.2d 1112 (2d Cir. 1992) .....	13
<u>United States v. Roldan-Zapata</u> , 916 F.2d 795 (2d Cir. 1990).....	15
<u>United States v. Russo</u> , 302 F.3d 37 (2d Cir. 2002).....	18
<u>United States v. Tarricone</u> , 996 F.2d 1414 (2d Cir. 1993) .....	13
<u>United States v. Tracy</u> , 12 F.3d 1186 (2d Cir. 1993).....	17, 19
<u>United States v. Vallejos</u> , 742 F.3d 902 (9th Cir. 2014) .....	9
<u>United States v. Williams</u> , 930 F.3d 44 (2d Cir. 2019) .....	9
<u>United States v. Zackson</u> , 12 F.3d 1178 (2d Cir. 1993) .....	14

#### STATUTES

18 U.S.C. § 1343.....	4
18 U.S.C. § 1349.....	4
18 U.S.C. § 1956(h).....	4
18 U.S.C. § 1957.....	4

#### RULES

Federal Rule of Evidence 403.....	7, 16
Federal Rule of Evidence 404(b).....	passim
Federal Rule of Evidence 801.....	8, 10, 11, 12
Federal Rule of Criminal Procedure 16 .....	13, 14, 15, 16

PRELIMINARY STATEMENT

The defendant is charged in a four-count superseding indictment with wire fraud conspiracy, wire fraud, money laundering conspiracy, and money laundering, for perpetrating a multimillion-dollar scheme to defraud U.S. businesses in the online digital advertising industry. Trial is scheduled to proceed in November, with jury selection on November 23, 2020, and opening statements on November 30, 2020.

The government now sets forth additional motions in limine for the admission of certain evidence at trial and for additional disclosures from the defense. Specifically, the government moves: (i) to admit additional evidence of the defendant's other acts pursuant to Federal Rule of Evidence 404(b); (ii) to admit additional statements of the defendant's co-conspirators made in furtherance of the conspiracy; (iii) to compel additional disclosures related to the defense expert; and (iv) to admit evidence of a prior criminal conviction during the cross-examination of the defense expert.

## BACKGROUND

On December 20, 2016, researchers at a private cybersecurity firm based in New York, New York, published a white paper titled “The Methbot Operation,” revealing the operation of an online digital advertising fraud scheme. In the white paper, the cybersecurity firm revealed the Internet Protocol (“IP”) addresses of computers used to carry out the fraud (the “Malicious IPs”). The cybersecurity firm explained that, based on its monitoring of network traffic related to advertisement impressions on behalf of various advertising clients, it had observed computers associated with the Malicious IPs transmitting false data to create the impression that a real human internet user was viewing an advertisement on a real internet webpage, when in fact a computer that was not controlled by any individual human (sometimes referred to as a “bot”) was loading the advertisement on a fake webpage. The cybersecurity firm further explained that the Malicious IPs were associated with false registration data in publicly available IP registration databases.

The Federal Bureau of Investigation (the “FBI”) began investigating the Malicious IPs and the scheme associated with them (the “Methbot scheme”). The investigation revealed that the defendant, ALEXANDR ZHUKOV, also known as “Alexander Zhukov” and “ibetters,” controlled the Malicious IPs. Specifically, the defendant leased the Malicious IPs from various IP address leasing companies and assigned those IPs to thousands of datacenter computer servers that he also controlled, and that were located in commercial datacenters in the United States and elsewhere. The defendant and his co-conspirators created false registration data for the Malicious IPs, making it appear that the Malicious IPs were associated with residential computers across the United States instead of datacenter computer servers in commercial datacenters.

The defendant and his co-conspirators then programmed the datacenter computer servers to simulate the internet activity of real human internet users, directing the servers to operate an automated browser, click on online advertisements a randomly determined number of times, simulate a mouse moving around and scrolling down a webpage, control and monitor video playback, falsely appear to be signed into popular social media services like Facebook, and circumvent fraud detection software deployed by certain U.S. cybersecurity firms. In this way, the defendant and his co-conspirators created “fraudulent ad traffic”—employing the datacenter computer servers to load fabricated webpages, offer up advertising space on fabricated webpages for bidding, load advertisements on the fabricated webpages through an automated computer program, and reap the resulting revenue. The defendant and his co-conspirators monitored the activity of the datacenter computer servers using an online control panel at a specific domain (centbycent.com); an email account associated with the domain sent regular emails to the defendant and his co-conspirators reporting on the performance of the thousands of datacenter computer servers employed in the scheme and the millions of fraudulent advertising impressions they created.

The defendant funneled his fraudulent ad traffic to others in the online digital advertising industry under the cover of his ad network Media Methane. The defendant represented that Media Methane delivered advertisements to real human internet users accessing real internet webpages, when in fact it merely delivered advertisements to the defendant’s datacenter computer servers. The defendant made millions of dollars from the

scheme. He moved the resulting proceeds through multiple corporate bank accounts located around the world and re-invested some of the proceeds to perpetuate the fraud.

On November 6, 2018, the defendant was arrested by Bulgarian law enforcement authorities in Varna, Bulgaria, pursuant to a U.S. provisional arrest warrant based on a complaint charging him with wire fraud conspiracy (in violation of 18 U.S.C. § 1349). On January 18, 2019, the defendant was extradited to the United States based on an indictment charging him with wire fraud conspiracy (in violation of 18 U.S.C. § 1349), wire fraud (in violation of 18 U.S.C. § 1343), money laundering conspiracy (in violation of 18 U.S.C. § 1956(h)), and money laundering (in violation of 18 U.S.C. § 1957).

## ARGUMENT

### I. The Court Should Admit Evidence of the Defendant's Other Acts Pursuant to Federal Rule of Evidence 404(b)

#### A. Relevant Facts

In the government's first motion in limine, see ECF No. 94 at 11-15, the government provided notice that it seeks to introduce certain evidence of the defendant's other acts pursuant to Federal Rule of Evidence 404(b), including a chat related to the defendant's use of bots in connection with his operation of an online sports betting exchange. In that chat, the defendant explained to an interlocutor that he could not afford to pay for data feeds regarding sporting scores, so he was instead using bots to "crawl" other websites which posted those scores, copying the data for his own use.

The government now seeks to introduce another chat related to the defendant's use of bots to obtain data for his sports betting exchange. In this chat, appended hereto as Exhibit A and dated June 17, 2014, the defendant advertised his services as a "software provider" to a prospective customer ("Customer-1"). The defendant told Customer-1 that, without the defendant's help, Customer-1 would be reliant on commercial providers of sports betting data: "usually if your [sic] run your [sic] bookie you must to have [] providers . . . if you wanna have better data you have to purchase it from data provider." Referring to Betradar, a sports gambling data provider, Customer-1 asked: "so betradar is one of data providers? are you integrated with them? so with betradar I can have statistics and more betting options ?" The defendant then responded: "no . . . we steal data bro," followed by a "laughing" emoji. The defendant proceeded by stating that with his service, Customer-1 could "sa[v]e HUGE amount of money." Customer-1 asked, "what if the one who is being

robbed will find out? . . . won't the whole site crash then." The defendant replied, "we steal if for 2 years already [] and steal by farm of bots. It is our own solution. It is private info ) only u and me know about that."

The government moves in limine to admit this evidence of the defendant's other acts as evidence of his intent, preparation, knowledge, and absence of mistake.

B. Legal Standards

Federal Rule of Evidence 404(b) provides that evidence of "other crimes, wrongs or acts" may not be admitted to prove bad character, but may be admissible for other purposes, such as to prove "motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident." Fed. R. Evid. 404(b). The standards governing the admissibility of evidence under Rule 404(b) are well established:

First, the district court must determine if the evidence is offered for a proper purpose, one other than to prove the defendant's bad character or criminal propensity. If the evidence is offered for a proper purpose, the district court must next determine if the evidence is relevant to an issue in the case, and, if relevant, whether its probative value is substantially outweighed by the danger of unfair prejudice. Finally, upon request, the district court must give an appropriate limiting instruction to the jury.

United States v. Pitre, 960 F.2d 1112, 1119 (2d Cir. 1992) (citation omitted); see also Huddleston v. United States, 485 U.S. 681, 685 (1988); United States v. Tarricone, 996 F.2d 1414, 1421 (2d Cir. 1993).

Although under Rule 404(b) evidence of other crimes or wrongs is "not admissible to prove the character of a person in order to show action in conformity therewith, [the Rule] . . . permits admission of such evidence for other purposes, such as to show knowledge or intent." United States v. Aminy, 15 F.3d 258, 260 (2d Cir. 1994); Huddleston,

485 U.S. at 687-88. The Second Circuit has long viewed Rule 404(b) as an inclusive rule allowing “other acts” evidence if the evidence is offered to prove something other than criminal propensity, is relevant to the crime for which the defendant stands trial, and satisfies the balancing test of Federal Rule of Evidence 403. See, e.g., United States v. Carboni, 204 F.3d 39, 44 (2d Cir. 2000); United States v. Germosen, 139 F.3d 120, 127 (2d Cir. 1998).

C. Discussion

The government should be permitted to admit the above-referenced chat pursuant to Rule 404(b) as evidence of the defendant’s intent, preparation, knowledge, and absence of mistake.

Like the prior chat on this subject, this evidence is admissible because it demonstrates the defendant’s familiarity with bots and early use of bots to gather information online by impersonating human users, years before the start of the charged conspiracy—demonstrating that the defendant had the technical knowledge and preparation required to carry out the charged scheme. It similarly makes clear that the defendant understood that using bots to impersonate human users at scale was wrong and criminal (“we steal data”). In addition, as with the prior such chat that the government sought to introduce, the conduct described in this chat is not more serious than the charged conduct and therefore does not pose undue prejudice.

Indeed, counter to the argument in the defendant’s response to the government’s prior motion in limine (see ECF No. 108 at 2), the conduct described in this chat is technically quite similar to the charged scheme. It involves the use of computers that are programmed to engage in human activity (in both cases, browsing websites) in order to deceive online actors into believing that the computers’ activity is human, for the economic

benefit of the defendant and his co-conspirators. As such, this evidence is admissible pursuant to Rule 404(b).

II. The Court Should Admit the LinkedIn Profiles of Certain of the Defendant's Uncharged Co-Conspirators

A. Relevant Facts

The government's evidence at trial will include chats and emails written by employees of advertising companies other than Media Methane, including an advertising company based in the United States, referred to herein as "Company-1." Company-1 was an ad network that provided services to advertisers and advertising agencies. Certain Company-1 employees are unindicted co-conspirators of the defendant: they placed their clients' advertisements on the defendant's network, knowing that the advertisements would not be shown to real human internet users, and passed client funds to the defendant.

Most of the statements by Company-1 employees that the government will seek to introduce were made in the context of back-and-forth exchanges with the defendant and are nonhearsay because they are being offered for context and are necessary to render the defendant's statements intelligible. See Fed. R. Evid. 801(d)(2)(A); United States v. Sorrentino, 72 F.3d 294, 298 (2d Cir. 1995).

However, the government will also seek to introduce the LinkedIn profiles of two Company-1 employees: an individual ("Individual-1") who at the time of the charged conspiracy was the director of Company-1's Publisher Department; and a second individual ("Individual-2") who at the time of the charged conspiracy was a business development executive for Company-1. Individual-1 and Individual-2 assisted the defendant by keeping him informed about the degree to which Company-1's customers and advertising security vendors were able to detect the fraudulent nature of the defendant's advertising traffic. For example:

- On or about May 20, 2015, Individual-1 sent the defendant a Skype message advising him to “Load the player into several site pages, up to 5; the important thing is to send traffic to the first page, have it hanging in there for one minute, and then transfer it to the next one that has a player, and so on. This way you monetize 1 click 5 times.”
- On or about September 22, 2015, Individual-1 sent a Skype message to the defendant noting that “your streaming is way too obvious” and advising the defendant to “add more domains to diffuse the traffic.”
- On or about November 5, 2015, Individual-2 sent the defendant a list of hundreds of prominent website URLs, adding: “[T]his is the polished list . . . let’s use it now.”
- On or about October 12, 2016, Individual-2 sent the defendant a message asking: “So, are you spoofing any domains there in real time?” Individual-2 then asked the defendant to tell “Borya” to “crank up the . . . volume”—an apparent reference to Boris Timokhin, one of the defendant’s charged co-conspirators who helped to create the computer code for the defendant’s scheme.

Both Individual-1 and Individual-2 had LinkedIn profiles. LinkedIn has indicated that Individual-1 registered his LinkedIn account on January 25, 2013, and Individual-2 registered his LinkedIn account on September 25, 2012. Individual-1’s LinkedIn profile, as it existed in mid-2017, proclaimed that Company-1 was “focused on video advertising” and that it would “facilitate the balance between major advertisers [and] top ad networks.” The profile further claimed that Company-1 worked with “hundreds of direct advertisers.” Individual-2’s LinkedIn profile in mid-2017 described him as a “Business Development

Executive” at Company-1 and contained a third-party “recommendation” describing him as “a very responsible and hardworking person” with “high quality standards.”

The government moves in limine to admit the LinkedIn profiles of Individual-1 and Individual-2 statements made by co-conspirators in furtherance of the conspiracy and, in the alternative, as non-hearsay.

B. Legal Standards

A statement is not hearsay if the “statement is offered against a party and is . . . [made] by a co-conspirator of a party during the course and in furtherance of the conspiracy.” In re Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 93, 137 (2d Cir. 2008) (quoting Fed. R. Evid. 801(d)(2)(E)). The existence of a conspiracy and the declarant’s participation in that conspiracy are “preliminary questions of fact” to be resolved by the district court by applying a preponderance of the evidence standard. Id. The “hearsay statement itself may be considered in establishing the existence of the conspiracy,” and “there must be some independent corroborating evidence of the defendant’s participation in the conspiracy.” United States v. Gigante, 166 F.3d 75, 82 (2d Cir. 1999) (internal marks omitted).

For statements to be “in furtherance” of the conspiracy, the Second Circuit has explained that:

the statements must in some way have been designed to promote or facilitate achievement of the goals of the ongoing conspiracy, as by, for example, providing reassurance to a co-conspirator, seeking to induce a co-conspirator’s assistance, serving to foster trust and cohesiveness, or informing co-conspirators as to the progress or status of the conspiracy, or by prompting the listener — who need not be a co-conspirator — to respond in a way that promotes or facilitates the carrying out of a criminal activity.

United States v. Tracy, 12 F.3d 1186, 1196 (2d Cir. 1993) (internal citations omitted); see also In re Terrorist Bombings, 552 F.3d at 139. A statement is also made in furtherance of a conspiracy where the statement provides “information regarding the current status of the conspiracy and its membership.” United States v. Fawwaz, No. 15 CR 1731, 2017 WL 2399329, at \*3 (2d Cir. June 2, 2017) (internal marks omitted); see also United States v. Russo, 302 F.3d 37, 46 (2d Cir. 2002) (collecting cases) (“The operation of [a criminal conspiracy] requires that information be passed among interested persons, advising them of the membership and the hierarchy.”). Importantly, “[t]hough the Rule requires that both the declarant and the party against whom the statement is offered be members of the conspiracy, there is no requirement that the person to whom the statement is made also be a member.” United States v. Beech-Nut Nutrition Corp., 871 F.2d 1181, 1199 (2d Cir. 1989) (citation omitted).

In addition to the above, a statement is not hearsay where it is not offered for its truth. See United States v. Dupree, 706 F.3d 131, 136 (2d Cir. 2013) (“[I]f the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted, and the statement is not hearsay.” (quoting advisory committee's note to Fed. R. Evid 801(c)).

### C. Discussion

The government should be permitted to admit the LinkedIn profiles of uncharged co-conspirators Individual-1 and Individual-2 because those communications were made in furtherance of the conspiracy.

As a preliminary matter, the evidence makes plain that Individual-1 and Individual-2 participated in a conspiracy with the defendant. As set forth above, both

individuals knowingly assisted the defendant in refining his fraudulent ad traffic so that it would bypass automated anti-fraud filters, and then paid the defendant for that traffic using money from Company-1's clients.

Furthermore, Individual-1 and Individual-2 used their LinkedIn profiles in furtherance of the conspiracy to attract clients (and, thus, potential victims) to use Company-1 to place advertisements. By proclaiming that Company-1 was "focused on video advertising" and that it would "facilitate the balance between major advertisers [and] top ad networks," Individual-1's profile attracted advertisers to pay money to Company-1 for what they believed would be opportunities to show their advertisements to real human internet users visiting real websites. Similarly, Individual-2's profile, describing him as "a very responsible and hardworking person" with "high quality standards," furthered the fraudulent scheme by encouraging client-victims to enlist Individual-2's services and pay Company-1 for advertising opportunities. Therefore, these communications qualify as communications made in furtherance of the conspiracy. See Fed. R. Evid. 801(d)(2)(E).

In the alternative, the government seeks to offer both LinkedIn profiles for a nonhearsay purpose—specifically, to demonstrate what Individual-1 and Individual-2 were communicating to prospective victims and to the defendant. With respect to prospective victims, the statements by Individual-1 and Individual-2 that they worked for a company that could "facilitate the balance between major advertisers [and] top ad networks" is not being introduced for its truth but rather for its falsity, as both individuals were luring in corporate victims with false promises of placing ads online that would be viewed by real human internet users. With respect to the defendant, the statements by Individual-1 and Individual-2 about their roles at Company-1 are evidence of the defendant's state of mind and

understanding of whom he was communicating with about ad fraud. As such, the LinkedIn profiles of Individual-1 and Individual-2 are admissible because they are offered for a nonhearsay purpose. See Dupree, 706 F.3d at 136.

III. The Court Should Order the Defense to Provide a More Complete Expert Disclosure

A. Relevant Facts

On August 1, 2020, the defendant notified the government that he intends to call Kenneth Wong, an information technology executive, regarding “IT and advertising security and testing, internet fraud, the structure and function of internet bots, and the structure of the methbot.” This paltry disclosure does not satisfy the defendant’s disclosure requirements under Federal Rule of Criminal Procedure 16(b)(1)(C). Accordingly, the government moves the Court to order the defendant to provide a sufficient disclosure under Rule 16(b)(1)(C).

B. Legal Standards

Rule 16(b)(1)(C) requires that the defendant must, at the government’s request, give to the government a written summary of any testimony that the defendant intends to use under Rules 702, 703, or 705 of the Federal Rules of Evidence as evidence at trial.” Fed. R. Crim. P. 16(b)(1)(C), see also United States v. Yousef, 327 F.3d 56, 148 (2d Cir. 2003). “This summary must describe the witness’s opinions, the bases and reasons for those opinions, and the witness’s qualifications.” Id. The purpose of the expert disclosure requirement is to “minimize surprise that often results from unexpected expert testimony, reduce the need for continuances, and to provide the opponent with a fair opportunity to test the merit of the expert’s testimony through focused cross-examination.” Fed. R. Crim. P. 16, advisory committee’s note to 1993 amendment. Indeed, “[w]ith increased use of both

scientific and nonscientific expert testimony, one of counsel’s most basic discovery needs is to learn that an expert is expected to testify.” Id. A trial court has “broad discretion in fashioning a remedy,” for failure to comply with Rule 16, including granting a continuance, ordering the exclusion of evidence or fashioning any other remedy that is “just under the circumstances.” United States v. Lee, 834 F.3d 145, 158 (2d Cir. 2016); Fed. R. Crim. P. 16(d)(2)(A)-(D) (a district court may order “any other [remedy] that is just under the circumstances”).

To satisfy the Rule 16 standard, the required summary must do more than list “general” or “extremely broad topics on which the expert might opine,” and even a “more specific” summary is insufficient if it does not provide a true “summary” of the opinion and “identify the basis for that opinion.” United States v. Ulbricht, 858 F.3d 71, 115 (2d Cir. 2017).

### C. Discussion

Here, the defendant’s disclosure—which is quoted in its entirety above—clearly fails to meet the required threshold. Indeed, the defendant’s disclosure in this case is even less informative than the one at issue in Ulbricht, which was found to be “plainly inadequate”:

Both disclosures merely listed general and in some cases extremely broad topics on which the experts might opine. For example, the disclosures indicated that the experts would testify on general topics, including: “the origins of Bitcoin,” “the various purposes and uses of Bitcoin,” “the mechanics of Bitcoin transactions,” “the value of Bitcoin over time since its inception,” “the concepts of Bitcoin speculating and Bitcoin mining,” “[g]eneral principles of internet security and vulnerabilities,” the “import of some lines of PHP code provided to defense counsel in discovery,” and “[g]eneral principles of public-key

“cryptography,” among others...They did not summarize the experts’ opinions about those topics, let alone describe the bases for the experts’ opinions.

Id. Such is the case here. While the topics listed by the defendant in his disclosure generally pertain to issues in the case, the disclosure is “so vague that it is difficult to discern whether the proffered expert testimony would [be] at all relevant” under Rules 401 and 702(a) of the Federal Rules of Evidence. Id.

Accordingly, the defendant should be ordered to provide a disclosure that comports with Rule 16(b)(1)(C) and describe what opinions the proposed expert will offer and the methodology used to arrive at those conclusions.

IV. The Court Should Permit the Government to Cross-Examine the Defense Expert On His Prior Conviction

A. Relevant Facts

On September 19, 1997, Mr. Wong was arrested on charges of grand larceny in the third degree, in violation of New York Penal Law § 155.35, a class D felony, and criminal possession of stolen property in the third degree, in violation of New York Penal Law § 165.50, a class D felony misdemeanor. The arrest resulted from Mr. Wong’s theft of a new IBM ThinkPad laptop computer from IBM’s facilities in Thornwood, New York. At the time, Mr. Wong was a co-op employee at IBM. The computer was valued at approximately \$3,500. On the day of his arrest, Mr. Wong waived his Miranda rights and confessed orally and in writing to stealing the IBM laptop computer a few months earlier. Mr. Wong resolved his case by subsequently pleading guilty to criminal possession of stolen property in the fifth degree, in violation of New York Penal Law § 165.40, a class A misdemeanor. Mr. Wong was sentenced to probation.

Assuming the defendant remedies his Rule 16(b)(1)(C) disclosure and Mr. Wong's proposed expert testimony is deemed relevant and admissible, the government hereby provides notice of its intent to use Mr. Wong's prior criminal conviction, dated April 9, 1998, for criminal possession of stolen property in the fifth degree, during its cross-examination of Mr. Wong. As such, the government requests that the Court permit the government, on cross-examination, to: (i) pursuant to Rule 608, inquire into the specific instance of theft committed by Mr. Wong; and (ii) pursuant to Rule 609, introduce evidence of Mr. Wong's resulting criminal conviction.

B. Legal Standards

Federal Rules of Evidence 608 and 609 govern the admissibility of evidence of prior convictions for impeachment purposes. As relevant here, evidence of a prior felony conviction "must be admitted, subject to Rule 403...in a criminal case in which the witness is not a defendant." Fed. R. Evid. 609(a)(1)(A). Under Rule 609(a)(1), the "evidence" of prior convictions that may be admitted includes "the essential facts of a witness's convictions, including the statutory name of each offense, the date of conviction, and the sentence imposed." United States v. Estrada, 430 F.3d 606, 615 (2d Cir. 2005); see also United States v. Brown, 606 F. Supp. 2d 306, 315-16 (E.D.N.Y. 2009) (same).

In conducting the Rule 403 analysis and weighing the probative versus prejudicial value of impeaching a defendant with a prior conviction, courts generally consider several factors, including: (1) the impeachment value of the prior crimes; (2) the date of the convictions and the defendant's subsequent history; (3) the degree of similarity between the past crimes and the charged crime, with dissimilarity favoring admission; (4) the importance of the witness's testimony; and (5) the centrality of the credibility issue. See

United States v. Hayes, 553 F.2d 824, 828 (2d Cir. 1977); see also United States v. Jimenez, 214 F.3d 1095, 1098 (9th Cir. 2000); United States v. Smith, 131 F.3d 685, 687 (7th Cir. 1997); United States v. Sloman, 909 F.2d 176, 181 (6th Cir. 1990); Jones v. City of New York, No. 98 Civ. 6493 (LBS), 2002 WL 207008, at \*2 (S.D.N.Y. Feb. 11, 2002).

If the later of a conviction or the date of the defendant's release from confinement for that conviction is more than ten years old, then, pursuant to Rule 609(b), evidence of the conviction is admissible only if "its probative value, supported by specific facts and circumstances, substantially outweighs its prejudicial effect" and the party seeking to offer it gives the opposing party reasonable written notice of its intent to use the evidence. Courts apply the same balancing test as that prescribed by Rule 609(a), but the heightened standard of Rule 609(b) requires that the evidence have more probative value than that required under Rule 609(a). See Brown, 606 F. Supp. 2d at 313. In addition, under Rule 609(b), a court must "make an on-the-record finding based on specific facts and circumstances that the probative value of the evidence substantially outweighs the danger of unfair prejudice." Jones v. N.Y. City Health & Hosps. Corp., 102 F. App'x 223, 226 (2d Cir. 2004) (summary order); see also United States v. Payton, 159 F.3d 49, 57-58 (2d Cir. 1998) (upholding district court's decision to admit defense witness's 13-year-old convictions where court specifically found that witness's "credibility was "crucial"; the impeachment value of her convictions was substantial; and the government provided defendant with sufficient advance notice of its intent to use these convictions in her cross-examination").

#### C. Discussion

Mr. Wong's prior conviction, and the facts and circumstances surrounding that conviction, are highly probative of his credibility, honesty, and character for truthfulness, and

have considerable impeachment value in this case. While the conviction is remote in time, it “is settled in this Circuit that a conviction for criminal possession of stolen property is ‘probative evidence on the issue of credibility.’” Sango v. City of New York, No. 83-CV-5177, 1989 WL 86995, at \*17 (E.D.N.Y. July 25, 1989) (quoting United States v. Reed, 526 F.2d 740, 743 (2d Cir. 1975)) (discussing misdemeanor conviction); see United States v. Thomas, 214 F. Supp. 3d 187, 196 (E.D.N.Y. 2016) (Kuntz, J.) (noting that “courts in the Second Circuit have held crimes involving theft, robbery, and burglary particularly probative of veracity because they rest on dishonest conduct” (citing cases)); United States v. White, No. 08-CR-682, 2009 WL 4730234, at \*3 (E.D.N.Y. 2009) (Garaufis, J.) (noting that in “particular, theft crimes, and other crimes involving stealth bear on a witness’s propensity to testify truthfully” and that the “theft element is probative of honesty”); see also United States v. Walia, No. 14-CR-213, 2014 WL 3734522, at \*15 (E.D.N.Y. July 25, 2014) (Brodie, J.) (holding that, under Rule 608(b), the government could cross-examine the defendant about his arrest for, *inter alia*, criminal possession of stolen property because “[s]uch conduct is probative of [his] character for truthfulness or untruthfulness” (citing cases)); United States v. Brown, No. 07-CR-874, 2009 WL 497606, at \*3 (E.D.N.Y. Feb. 26, 2009) (Matsumoto, J.) (suggesting, in connection with Rule 608(b), that “forgery, perjury, or fraud” would “directly reveal truthfulness”); United States v. Haouari, No. 00- CR-015, 2001 WL 1586676, at \*2 (S.D.N.Y. Dec. 11, 2001) (noting the fact that the witness had previously stolen computers as relevant to the witness’s credibility).

Here, the probative value is particularly compelling because of the specific facts and circumstances surrounding Mr. Wong’s prior conviction and the purposes for Mr. Wong’s testimony in this case. First, Mr. Wong stole an IBM computer while working for

IBM—that is, that he committed a breach of trust by stealing property from his employer. Second, Mr. Wong stole the computer several months before his arrest and took no actions to return it until caught by the police. Third, the computer was valued at \$3,500. These factors all bear on the relative importance Mr. Wong would place on his oath to tell the truth as a witness: his crime directly shows a willingness to lie and deceive in order to benefit himself.

This is exactly the type of impeachment material that the jury must hear in order to fairly evaluate Mr. Wong's credibility. Such impeachment does not unfairly prejudice the defendant, as the impeachment pertains to the prior conduct of a hired expert, and not the conduct of the defendant or one of his co-conspirators. Nor does such impeachment unfairly prejudice the defendant's expert: the defense will have an opportunity during direct examination to elicit Mr. Wong's education, employment, and expertise in computer-related fields; permitting the government to question him about his deceptive conduct during one of those instances of employment is equitable and essential for the jury to make an informed credibility determination. For these reasons, and significantly, the district court in United States v. Gasperini, No. 16-CR-441 (E.D.N.Y. 2017) (NGG), permitted the government to cross-examine Mr. Wong on his prior criminal conduct, and this Court should as well.

CONCLUSION

For the foregoing reasons, the government respectfully requests that the Court grant the government's motions in advance of trial.

Dated: Brooklyn, New York  
October 5, 2020

Respectfully submitted,

SETH D. DUCHARME  
Acting United States Attorney  
Eastern District of New York  
271 Cadman Plaza East  
Brooklyn, New York 11201

By: \_\_\_\_\_/s/  
Saritha Komatireddy  
J. Artie McConnell  
Alexander F. Mindlin  
Assistant United States Attorneys  
(718) 254-7000